TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Liisa Lampinen

Rationaaliluvun desimaaliesitys algebrallisesta ja lukuteoreettisesta näkökulmasta

Informaatiotieteiden yksikkö
Matematiikka
Kesäkuu 2016

Tampereen yliopisto
Informaatiotieteiden yksikkö
LAMPINEN, LIISA: Rationaaliluvun desimaaliesitys algebrallisesta ja lukuteoreettisesta näkökulmasta
Pro gradu -tutkielma, 29 s.
Matematiikka
Kesäkuu 2016

Tiivistelmä

Tässä tutkielmassa on käsitelty rationaaliluvun desimaaliesitystä algebrallisesta ja lukuteoreettisesta näkökulmasta. Rationaaliluvun desimaaliesitys voi olla joko päättyvä tai jaksollinen. Mikäli desimaaliesitys ei ole päättyvä eikä jaksollinen, kyseessä ei ole rationaaliluku. Jaksollisen desimaaliesityksen jakso voi alkaa heti desimaalipilkun jälkeen tai desimaaliesityksessä voi olla esijakso. Rationaaliluvun desimaaliesitys määräytyy supistetussa muodossa olevan rationaaliluvun nimittäjän ominaisuuksien perusteella. Mikäli rationaaliluvun nimittäjän alkutekijähajotelmassa on ainoastaan kantaluvun 10 tekijöitä, on rationaaliluvun desimaaliesitys päättyvä. Mikäli rationaaliluvun osoittaja ja nimittäjä ovat keskenään jaottomia eikä nimittäjän alkutekijähajotelmassa ole kantaluvun 10 tekijöitä, on rationaaliluvun desimaaliesitys jaksollinen, ja jakso alkaa heti desimaalipilkun jälkeen. Rationaaliluvun desimaaliesitykseen sisältyy esijakso, mikäli rationaaliluvun nimittäjän alkutekijähajotelmassa on kantaluvun 10 tekijöiden lisäksi myös muita tekijöitä. Tässä tutkielmassa on myös tarkasteltu rationaaliluvun jakokulmalaskun jakojäännöksiä tapauksessa, jossa rationaaliluvun osoittaja on 1. Jakojäännösten muodostama jäännösluokkien joukko modulo b modulaarisen kertolaskun suhteen on alkuluokkien ryhmän modulo b aliryhmä, missä b on rationaaliluvun nimittäjä. Tapausta, jossa rationaaliluvun osoittaja on erisuuri kuin 1, on käsitelty tässä tutkielmassa ainoastaan esimerkin avulla.

Asiasanat: rationaaliluku, jaksollinen desimaaliesitys, päättyvä desimaaliesitys, alkuluokkaryhmä

Sisältö

1 Johdanto

Tässä tutkielmassa on käsitelty rationaaliluvun desimaaliesitystä algebrallisesta ja lukuteoreettisesta näkökulmasta.

Yliopistotason matematiikan perus- ja aineopinnot auttavat työn matemaattisen sisällön ymmärtämisessä. Aliluvussa 2.1 on esitetty tutkielman kannalta oleellisia taustatietoja määritelmien ja lauseiden muodossa helpottamaan lukijaa tutkielman seuraamisessa. Tämän luvun tuloksia ei ole todistettu, lukija voi perehtyä todistuksiin esimerkiksi työssä käytettyjen lähdeteosten avulla. Varsinaisessa tutkielmaosassa on esitetty tutkielmaan lähemmin liittyviä lauseita. Valtaosa näistä tuloksista on todistettu tutkielmassa.

Tässä tulkielmassa on käsitelty supistetussa muodossa olevan rationaaliluvun $\alpha = \frac{r}{s} = \frac{r}{TU}$, missä $T = 2^u 5^v$, missä $u, v = 0, 1, 2, 3 \ldots$, ja $\text{syt}(r, s) = \text{syt}(10, U) = 1$, desimaaliesitystä. Luku T sisältää kaikki luvun s alkutekijähajotelman tekijät 2 ja 5, eli kantaluvun 10 tekijät, ja muut alkutekijät sisältyvät lukuun U.

Aliluvuissa 3.1 sekä 3.2 on määritelty rationaaliluku sekä päättyvä ja jaksollinen desimaaliesitys. Aliluvussa 3.2 on tarkasteltu tarkemmin rationaaliluvun desimaaliesitystä. Aliluvussa on esitetty, milloin rationaaliluvun desimaaliesitys on päättyvä ja milloin jaksollinen. Mikäli desimaaliesitys ei ole päättyvä eikä jaksollinen, kyseessä ei ole rationaaliluku. Rationaaliluvun desimaaliesitys on päättyvä, mikäli $U = 1$, eli rationaaliluku on muotoa $\alpha = \frac{r}{s} = \frac{r}{T} = \frac{r}{2^u 5^v}$, missä $u, v = 0, 1, 2, \ldots$, eli luvun s kaikki alkutekijät jakavat kantaluvun 10. Mikäli $U \neq 1$, rationaaliluvun desimaaliesitys on päättymätön. Tällöin desimaaliesitys on jaksollinen. Desimaaliesityksen jakso voi alkaa heti desimaalipilkun jälkeen, tai desimaaliesityksessä on esijakso. Esijakson pituus N määräytyy luvun T alkutekijöiden 2 ja 5 potensseista u ja v siten, että esijakson pituus $N = \max\{u, v\}$. Desimaaliesityksen jaksonpituus $\lambda = \text{ord}_U 10$. Näin ollen rationaaliluvun osoittaja ei vaikuta jaksonpituuteen eikä esijakson pituuteen. Lisäksi huomataan, että esijakson pituus ei riipu luvusta U eikä jaksonpituus riipu luvusta T. Aliluvussa on esitetty todistukset desimaaliesityksen jaksonpituudelle sekä esijakson pituudelle.

Aliluvussa 3.3 on todettu, että alkuluokkien joukko $\mathbb{Z}_m^\times$ varustettuna modulaarisella kertolaskulla $\otimes$ on Abelin ryhmä. Muotoa $\frac{1}{b}$, missä $\text{syt}(b, 10) = 1$, olevan rationaaliluvun jakokulmalaskun jakojäännöksien $r_n, n = 0, 1, 2, \ldots$, muodostama jäännösluokkien joukko modulo b on alkuluokkien ryhmän modulo b aliryhmä. Muotoa $\frac{1}{b}$, missä $\text{syt}(b, 10) = 1$, olevan rationaaliluvun jakojäännösten $r_n, n = 0, 1, 2, \ldots$, muodostaman jonon jaksonpituus l on yhtäsuuri kuin rationaaliluvun desimaaliesityksen jaksonpituus λ. Huomataan myös, että jaksonpituus λ jakaa Eulerin ϕ-funktion arvon $\phi(b)$. Muotoa $\frac{c}{b}$ olevaa rationaalilukua on tässä työssä käsitelty ainoastaan esimerkin avulla. Esimerkistä huomataan, että mikäli alkiot $[1]_b$ ja $[c]_b$ kuuluvat samaan ryhmän $\mathbb{Z}_b^\times$ sivuluokkaan, ovat rationaalilukujen $\frac{1}{c}$ sekä $\frac{b}{c}$ jakojäännökset keskenään samat, joten niiden desimaaliesityksien jaksot muodostuvat samoista luvuista, jotka esiintyvät samassa järjestyksessä. Jakson ensimmäinen luku määräytyy ensimmäisen jakojäännöksen perusteella.

Tutkielman pääasiallisina lähdeteoksina on käytetty Kenneth H. Rosenin *Elementary Number Theory and Its Applications* -teosta sekä Jaska Porasen ja Pentti Haukkasen Matematiikkalehti Solmussa julkaistua artikkelia *Jaksolliset desimaaliesitykset algebrallisesta näkökulmasta*. Muita lähteitä on käytetty pääasiassa täydentämään näitä kahta päälähdettä.

2 Valmistelevia tarkasteluja

2.1 Tarvittavien käsitteiden määritelmiä ja merkintöjä

Määritelmä 2.1. [7, s. 20] Reaaliluvun x *kokonaisosa* on suurin kokonaisluku, joka on pienempi tai yhtäsuuri kuin luku x. Kokonaisosasta käytetään merkintää $[x]$.

Esimerkki 2.1. Reaalilukujen $3,9$; 4 ja $-7,2$ kokonaisosat ovat seuraavat:

$$[3,9] = 3, \qquad [4] = 4, \qquad [-7,2] = -8.$$

Määritelmä 2.2. [7, s. 338] Reaaliluvun γ *desimaaliesitys* $\gamma = 0, q_1 q_2 q_3 \ldots$ muodostuu jonosta q_k, joka määritellään jonon γ_k avulla seuraavasti:

$$\begin{aligned} \gamma_k &= 10\gamma_{k-1} - [10\gamma_{k-1}] \\ q_k &= [10\gamma_{k-1}] \\ \gamma_0 &= \gamma, \end{aligned}$$

missä $k = 1, 2, \ldots$

Esimerkki 2.2. Esimerkiksi reaaliluvun $\gamma = 0,12345\ldots$ desimaaliesityksen laskemiseksi käytetään seuraavia jonoja:

$$\begin{aligned} \gamma_0 &= 0,12345\ldots \\ \gamma_1 &= 10\gamma_0 - [10\gamma_0] = 10 \cdot 0,12345\ldots - [10 \cdot 0,12345\cdots] \\ &= 1,2345\cdots - 1 = 0,2345\cdots \\ \gamma_2 &= 10\gamma_1 - [10\gamma_1] = 10 \cdot 0,2345\cdots - [10 \cdot 0,2345\cdots] \\ &= 2,345\cdots - 2 = 0,345\cdots \\ &\vdots \\ q_1 &= [10\gamma_0] = [10 \cdot 0,12345\cdots] = [1,2345\cdots] = 1 \\ q_2 &= [10\gamma_1] = [10 \cdot 0,2345\ldots] = 2 \\ &\vdots \end{aligned}$$

Lause 2.1. Euler-Fermat'n lause: *Jos* $\mathrm{syt}(a, m) = 1$*, niin*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Todistus. Todistus sivuutetaan. Ks. [3, s. 5]. □

Määritelmä 2.3. [7, s. 232] Olkoot luvut a ja m, $m \geq 2$, keskenään jaottomia kokonaislukuja. Lukua x sanotaan luvun a *kertaluvuks*i modulo m, kun x on pienin sellainen positiivinen kokonaisluku, että $a^x \equiv 1 \pmod{m}$. Kertaluvusta käytetään merkintää $x = \mathrm{ord}_m a$.

Esimerkki 2.3. Luvun 4 kertaluku modulo 9 on 3, koska

$$\begin{aligned} 4^3 &\equiv 1 \pmod 9, \quad \text{ja} \\ 4^x &\not\equiv 1 \pmod 9, \quad \text{kun} \quad x = 1, 2. \end{aligned}$$

Lause 2.2. *Jos a ja m ovat keskenään jaottomia kokonaislukuja ja $m > 0$, niin luku $x > 0$ on kongruenssin $a^x \equiv 1 \pmod m$ ratkaisu, jos ja vain jos $\mathrm{ord}_m a \mid x$.*

Todistus. Todistus sivuutetaan. Ks. [7, s. 233]. □

Lause 2.3. *Olkoot $a, c \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Kongruenssiyhtälöllä $ax \equiv c \pmod m$ on kokonaislukuratkaisu, jos ja vain jos $\mathrm{syt}(a, m) \mid c$.*

Todistus. Todistus sivuutetaan. Ks. [4, s. 113]. □

Lause 2.4. Lagrangen lause: *Olkoon $(G, \star)$ äärellinen ryhmä, ja olkoon H sen aliryhmä. Tällöin joukon H alkioiden lukumäärä jakaa joukon G alkioiden lukumäärän*

$$|H| \Big| |G| .$$

Todistus. Todistus sivuutetaan. Ks. [2, s. 7]. □

Lause 2.5. *Olkoon $(G, \star)$ äärellinen ryhmä, ja olkoon H sen aliryhmä. Tällöin aliryhmän H määräämien sivuluokkien lukumäärä k on*

$$k = \frac{|G|}{|H|}.$$

Todistus. Todistus sivuutetaan. Ks. [2, s. 7]. □

3 Rationaaliluku ja desimaaliesitys

3.1 Rationaaliluku

Määritelmä 3.1. [7, s. 336] Reaaliluku α on *rationaaliluku*, jos $\alpha = \frac{a}{b}$, missä a ja b ovat kokonaislukuja sekä $b \neq 0$.

Rationaalilukujen joukolle käytetään merkintää $\mathbb{Q}$. Rationaalilukujen peruslaskutoimitukset antavat aina tulokseksi rationaaliluvun.

3.2 Desimaaliesitys

Määritelmä 3.2. [7, s. 341] Reaaliluvun $x = 0, q_1 q_2 q_3 \ldots$ desimaaliesitys on *päättyvä*, jos on olemassa sellainen positiivinen kokonaisluku n, että $q_n = q_{n+1} = q_{n+2} = \cdots = 0$.

Määritelmä 3.3. [7, s. 343] Reaaliluvun desimaaliesitys on *jaksollinen*, jos on olemassa sellaiset kokonaisluvut $N \geq 0$ ja $\lambda > 0$, että $q_{n+\lambda} = q_n$, kun $n > N$. Tällöin merkitään $x = 0, q_1 q_2 q_3 \ldots q_N \overline{q_{N+1} q_{N+2} \ldots q_{N+\lambda}}$. Tällöin $q_1 q_2 \ldots q_N$ on *esijakso*, ja *jakso* on $q_{N+1} q_{N+2} \ldots q_{N+\lambda}$, jonka *jaksonpituus* on λ.

Huomioitavaa on, että mikäli λ on rationaaliluvun desimaaliesityksen jaksonpituus, myös $t\lambda$, missä $t = 2, 3, \ldots$, on desimaaliesityksen jakso. Vastaavasti mikäli rationaaliluvun desimaaliesityksen esijakson pituus on N ja jaksonpituus λ, on myös $N + t\lambda$, missä $t = 1, 2, \ldots$, desimaaliesityksen esijakso. Selvyyden vuoksi jaksosta ja esijaksosta puhuttaessa tarkoitetaan pienimpiä jakson ja esijakson pituuksia.

Seuraavissa lauseissa tullaan osoittamaan, että supistetussa muodossa olevan rationaaliluvun desimaaliesityksen muoto riippuu ainoastaan rationaaliluvun $\alpha = \frac{r}{s}$ nimittäjästä s. Lauseissa luku $\frac{r}{s}$ on supistetussa muodossa, ja nimittäjä s esitetään muodossa $s = TU$, missä luku T muodostuu kantaluvun 10 alkutekijöistä, eli $T = 2^u 5^v$, missä $u, v = 0, 1, 2, \ldots$, ja $\text{syt}(U, 10) = 1$. Näin ollen luvussa U ei ole kantaluvun 10 alkutekijöitä tekijöinä. Mikäli $U = 1$, nimittäjä s on muotoa $s = TU = T \cdot 1 = T = 2^u 5^v$. Tätä tapausta käsitellään lauseessa 3.1 sekä lauseen 3.2 kohdassa (i). Tapausta $U > 1$ käsitellään lauseen 3.2 kohdassa (ii) sekä lauseessa 3.3.

Lause 3.1. *Reaaliluvun α, $0 < \alpha < 1$, desimaaliesitys on päättyvä, jos ja vain jos α on rationaaliluku ja se on muotoa $\alpha = \frac{r}{s}$, missä* $\text{syt}(r, s) = 1$ *ja luvun s alkutekijät jakavat kantaluvun 10.*

Todistus. [7, s. 342] ” $\Longrightarrow$ ”: Oletetaan ensin, että luvulla α on päättyvä desimaaliesitys

$$\alpha = 0, q_1 q_2 q_3 \ldots q_n.$$

Tällöin luku α voidaan esittää muodossa

$$\begin{aligned}\alpha &= \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_n}{10^n} \\ &= \frac{q_1 \cdot 10^{n-1}}{10^n} + \frac{q_2 \cdot 10^{n-2}}{10^n} + \cdots + \frac{q_n}{10^n} \\ &= \frac{q_1 \cdot 10^{n-1} + q_2 \cdot 10^{n-2} + \cdots + q_n}{10^n}.\end{aligned}$$

Näin ollen luku α on rationaaliluku, jonka nimittäjässä on luku, joka voidaan esittää ainoastaan kantaluvun 10 alkutekijöiden tulona.

" $\Longleftarrow$ ": Oletetaan seuraavaksi, että $0 < \alpha < 1$, $\alpha = \frac{r}{s}$, missä $\text{syt}(r, s) = 1$ ja jokainen luvun s alkutekijä jakaa kantaluvun 10. Luku s on siis muotoa $s = 2^u 5^v$, missä $u, v = 0, 1, 2, \ldots$ Olkoon luku N luvun s alkutekijähajotelman korkein asteluku, eli $N = \max\{u, v\}$. Silloin luku s jakaa myös luvun 10^N. Koska $s \mid 10^N$, on luku 10^N muotoa $sa = 10^N$, ja myös a on positiivinen kokonaisluku. Tällöin

$$10^N \alpha = 10^N \frac{r}{s} = sa\frac{r}{s} = ar,$$

joten

$$\alpha = \frac{ar}{10^N}.$$

Luku ar on kokonaisluku, koska luvut a ja r ovat kokonaislukuja. Merkitään $ar = a_m a_{m-1} a_{m-2} \ldots a_1 a_0$. Nyt

$$\begin{aligned}\alpha = \frac{ar}{10^N} &= \frac{a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0}{10^N} \\ &= a_m 10^{m-N} + a_{m-1} 10^{(m-1)-N} + \cdots + a_1 10^{1-N} + a_0 10^{-N} \\ &= 0,00 \ldots 0 a_m a_{m-1} a_{m-2} \ldots a_1 a_0.\end{aligned}$$

Näin ollen luvulla α on päättyvä desimaaliesitys. □

Lauseen 3.1 perusteella rationaaliluvun desimaaliesitys on päättyvä, mikäli rationaaliluvun $\alpha = \frac{r}{s}$, missä $\text{syt}(r, s) = 1$, nimittäjän s ainoat alkutekijät ovat 2 ja 5, eli s on muotoa $s = 2^u 5^v$, missä $u, v = 0, 1, 2, \ldots$

Esimerkki 3.1. Esimerkkejä päättyvistä desimaaliesityksistä:

(i) Luvun $\frac{3}{40}$ desimaaliesitys $0,075$ on päättyvä, sillä luvulla 40 ei ole muita alkutekijöitä kuin luvut 2 ja 5:

$$40 = 2^3 5^1.$$

(ii) Luvun $\frac{7}{32}$ desimaaliesitys $0,21875$ on päättyvä, sillä

$$32 = 2^5 5^0.$$

Esimerkki 3.2. Esimerkkejä päättymättömistä desimaaliesityksistä:

(i) Luvun $\frac{5}{12}$ desimaaliesitys $0,416666\ldots$ ei ole päättyvä, sillä luvun 12 alkutekijähajotelma on

$$12 = 2^2 3^1$$

eikä lukua 12 voi esittää muodossa $2^u 5^v$.

(ii) Luvun $\frac{2}{9}$ desimaaliesitys $0,2222\ldots$ ei ole päättyvä, sillä luvun 9 alkutekijähajotelma on

$$9 = 3^2$$

eikä lukua 9 voi esittää muodossa $2^u 5^v$.

Desimaaliluvun jakso voi alkaa heti desimaalipilkun jälkeen, tai jaksoa voi edeltää esijakso.

Esimerkki 3.3. Esimerkkejä jaksoista ja esijaksoista:

(i) Desimaaliesitys

$$0,152152152\ldots = \frac{152}{999}$$

on jaksollinen, ja jakso 152 alkaa heti desimaalipilkun jälkeen.

(ii) Desimaaliesityksessä

$$0,82154545454\ldots = \frac{9037}{11000}$$

jakso 54 alkaa esijakson 821 jälkeen.

Lause 3.2. *Reaaliluku on rationaaliluku, jos ja vain jos sen desimaaliesitys on (i) päättyvä tai (ii) päättymätön ja jaksollinen.*

Todistus. [7, s. 344]
" $\Longleftarrow$ ":

(i) Oletetaan, että luvulla α on päättyvä desimaaliesitys. Lauseen 3.1 mukaan α on tällöin rationaaliluku.

(ii) Oletetaan, että luvun α desimaaliesitys on päättymätön ja jaksollinen. Merkitään desimaaliesityksen esijakson pituutta kirjaimella $N \geq 0$ ja jakson pituutta kirjaimella $\lambda \geq 1$. Tällöin

$$
\begin{aligned}
\alpha =& 0, q_1 q_2 \ldots q_N \overline{q_{N+1} q_{N+2} \ldots q_{N+\lambda}} \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_N}{10^N} + \frac{q_{N+1}}{10^{N+1}} + \cdots + \frac{q_{N+\lambda}}{10^{N+\lambda}} + \frac{q_{N+\lambda+1}}{10^{N+\lambda+1}} + \cdots + \frac{q_{N+\lambda+\lambda}}{10^{N+\lambda+\lambda}} \\
& + \frac{q_{N+2\lambda+1}}{10^{N+2\lambda+1}} + \cdots + \frac{q_{N+2\lambda+\lambda}}{10^{N+2\lambda+\lambda}} + \frac{q_{N+3\lambda+1}}{10^{N+3\lambda+1}} + \cdots \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_N}{10^N} + \left(\sum_{j=0}^{\infty} \left(\frac{1}{10^\lambda} \right)^j \right) \left(\frac{q_{N+1}}{10^{N+1}} + \cdots + \frac{q_{N+\lambda}}{10^{N+\lambda}} \right) \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_N}{10^N} + \frac{1}{1 - \frac{1}{10^\lambda}} \left(\frac{q_{N+1}}{10^{N+1}} + \cdots + \frac{q_{N+\lambda}}{10^{N+\lambda}} \right) \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_N}{10^N} + \frac{1}{\frac{10^\lambda - 1}{10^\lambda}} \left(\frac{q_{N+1}}{10^{N+1}} + \cdots + \frac{q_{N+\lambda}}{10^{N+\lambda}} \right) \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_N}{10^N} + \frac{10^\lambda}{10^\lambda - 1} \left(\frac{q_{N+1}}{10^{N+1}} + \cdots + \frac{q_{N+\lambda}}{10^{N+\lambda}} \right).
\end{aligned}
$$

Nyt jaksollinen desimaaliluku α on esitetty rationaalilukujen summana ja rationaalilukujen tulojen summana. Näin ollen voidaan todeta, että luku α on rationaaliluku.

" $\Longrightarrow$ ": Oletetaan seuraavaksi, että $0 < \alpha < 1$ on rationaaliluku, joka on muotoa $\alpha = \frac{r}{s} = \frac{r}{TU}$, missä $T = 2^u 5^v$, missä $u, v = 0, 1, 2 \ldots$, ja $\text{syt}(r, s) = \text{syt}(U, 10) = 1$.

(i) Mikäli $U = 1$, on rationaaliluku α muotoa $\alpha = \frac{r}{s} = \frac{r}{TU} = \frac{r}{T} = \frac{r}{2^u 5^v}$. Lauseessa 3.1 on osoitettu, että rationaaliluvun, jonka nimittäjän alkutekijät jakavat kantaluvun 10, desimaaliesitys on päättyvä.

(ii) Oletetaan seuraavaksi, että $U > 1$. Tällöin α on muotoa $\alpha = \frac{r}{s} = \frac{r}{TU}$. Olkoon luku N pienin sellainen kokonaisluku, että $T \mid 10^N$.

Koska T jakaa luvun 10^N, voidaan luku 10^N esittää muodossa $10^N = aT$, missä a on positiivinen kokonaisluku. Täten

$$
\begin{aligned}
10^N \alpha &= 10^N \frac{r}{s} \\
&= 10^N \frac{r}{TU} \\
&= aT \frac{r}{TU} \\
&= \frac{ar}{U}.
\end{aligned}
$$

Käytetään jakoyhtälöä (kts. lause 3.10) ja tietoa $0 < \alpha < 1$, jolloin saadaan

$$
\begin{aligned}
10^N \alpha &= \frac{ar}{U} \\
&= A + \frac{C}{U} \\
&< 10^N,
\end{aligned}
\tag{3.1}
$$

missä A ja C ovat kokonaislukuja siten, että $0 \leq A < 10^N$ ja $0 < C < U$ ja $\text{syt}(C, U) = 1$.

Olkoon λ luvun 10 kertaluku modulo U, ts. $\lambda = \text{ord}_U 10$. Määritelmän 2.3 perusteella $10^\lambda \equiv 1 \pmod{U}$, joten saadaan

$$10^\lambda \frac{C}{U} = (tU + 1)\frac{C}{U} = Ct + \frac{C}{U}, \tag{3.2}$$

missä t on kokonaisluku. Merkitään lukua $\frac{C}{U} < 1$ seuraavasti:

$$\frac{C}{U} = 0, c_1 c_2 c_3 \ldots c_\lambda + \frac{\gamma_\lambda}{10^\lambda},$$

missä

$$\begin{aligned} \gamma_k &= 10\gamma_{k-1} - [10\gamma_{k-1}] \\ c_k &= [10\gamma_{k-1}] \\ \gamma_0 &= \frac{C}{U}, \end{aligned} \tag{3.3}$$

missä $k = 1, 2, 3, \ldots$ Tällöin

$$\begin{aligned} 10^\lambda \frac{C}{U} &= 10^\lambda (0, c_1 c_2 c_3 \ldots c_\lambda + \frac{\gamma_\lambda}{10^\lambda}) \\ &= 10^\lambda \left(\frac{c_1}{10} + \frac{c_2}{10^2} + \frac{c_3}{10^3} + \cdots + \frac{c_\lambda}{10^\lambda} + \frac{\gamma_\lambda}{10^\lambda} \right) \\ &= 10^\lambda (c_1 10^{-1} + c_2 10^{-2} + c_3 10^{-3} + \cdots + c_\lambda 10^{-\lambda} + \gamma_\lambda 10^{-\lambda}) \\ &= (c_1 10^{\lambda-1} + c_2 10^{\lambda-2} + c_3 10^{\lambda-3} + \cdots + c_\lambda) + \gamma_\lambda. \end{aligned} \tag{3.4}$$

Merkitään luvun $10^\lambda \frac{C}{U}$ kaavoissa (3.2) ja (3.4) esiintyvät murto-osat yhtäsuuriksi ja huomioidaan, että $0 \leq \gamma_\lambda < 1$. Tästä seuraa, että

$$\gamma_\lambda = \frac{C}{U}.$$

Tästä seuraa kaavan (3.3) perusteella, että

$$\gamma_\lambda = \gamma_0.$$

Määritelmän 2.2 mukaan jono $q_k = [10\gamma_{k-1}]$ määritellään rekursiivisesti jonon γ_k

avulla. Kun $k = 1, 2, 3, \ldots, \lambda, \lambda+1, \lambda+2, \ldots$, saadaan

$$\begin{aligned}
\gamma_0 &= \gamma_\lambda & & \\
\gamma_1 &= 10\gamma_0 - [10\gamma_0] & q_1 &= [10\gamma_0] \\
\gamma_2 &= 10\gamma_1 - [10\gamma_1] & q_2 &= [10\gamma_1] \\
&\vdots & &\vdots \\
\gamma_\lambda &= 10\gamma_{\lambda-1} - [10_{\lambda-1}] & q_\lambda &= [10\gamma_{\lambda-1}] \\
\gamma_{\lambda+1} &= 10\gamma_\lambda - [10\gamma_\lambda] = 10\gamma_0 - [10\gamma_0] = \gamma_1 & q_{\lambda+1} &= [10\gamma_\lambda] = [10\gamma_0] = q_1 \\
\gamma_{\lambda+2} &= 10\gamma_{\lambda+1} - [10\gamma_{\lambda+1}] = 10\gamma_1 - [10\gamma_1] = \gamma_2 & q_{\lambda+2} &= [10\gamma_{\lambda+1}] = [10\gamma_1] = q_2 \\
&\vdots & &\vdots
\end{aligned}$$

Näin ollen $q_{\lambda+k} = q_k$, kun $k = 1, 2, 3, \ldots$. Täten luvulle $\frac{C}{U}$ saadaan jaksollinen desimaaliesitys

$$\frac{C}{U} = 0, q_1 q_2 \ldots q_\lambda q_1 q_2 \ldots q_\lambda q_1 \ldots = 0, \overline{q_1 q_2 \ldots q_\lambda}. \tag{3.5}$$

Merkitään, että kaavan (3.1) kokonaisluvun A esitys on $A = a_n a_{n-1} a_{n-2} \ldots a_1 a_0$. Yhdistetään kaavat (3.1) ja (3.5), jolloin saadaan

$$\begin{aligned}
10^N \alpha &= A + \frac{C}{U} \\
&= a_n a_{n-1} a_{n-2} \ldots a_1 a_0 + 0, \overline{q_1 q_2 \ldots q_\lambda} \\
&= a_n a_{n-1} a_{n-2} \ldots a_1 a_0, \overline{q_1 q_2 \ldots q_\lambda}.
\end{aligned}$$

Jaetaan puolittain luvulla 10^N, jolloin saadaan

$$\alpha = 0, 00 \ldots 0 a_n a_{n-1} a_{n-2} \ldots a_1 a_0 \overline{q_1 q_2 \ldots q_\lambda}.$$

Näin saatu luvun α desimaaliesitys on jaksollinen. Desimaaliesityksen esijakson pituus on N, esijakson alussa on $N-(n+1)$ nollaa ja jaksonpituus on $\lambda = \mathrm{ord}_U 10$. □

Lauseen 3.2 perusteella voidaan sanoa, onko jokin desimaaliluku rationaaliluku. Mikäli desimaaliluku on päättyvä tai jaksollinen, on kyseinen luku rationaaliluku lauseen 3.2 perusteella.

Esimerkki 3.4. Koska desimaaliluku $0, 25 = \frac{1}{4}$ on päättyvä ja desimaaliluku $0, \overline{745} = \frac{745}{999}$ on jaksollinen, ovat ne rationaalilukuja lauseen 3.2 perusteella.

Lause 3.3. *Olkoon α rationaaliluku, $0 < \alpha < 1$. Merkitään $\alpha = \frac{r}{s} = \frac{r}{TU}$, $\mathrm{syt}(r, s) = \mathrm{syt}(U, 10) = 1$. Kun $U > 1$, luvun α desimaaliesitys on päättymätön ja jaksollinen. Silloin esijakson pituus N on pienin sellainen positiivinen kokonaisluku, että $T \mid 10^N$ ja jaksonpituus on $\lambda = ord_U 10$.*

Todistus. [7, s. 346] Lauseen 3.2 (ii)-kohdassa on osoitettu, että mikäli $U > 1$, rationaaliluvulla on ainakin sellainen päättymätön ja jaksollinen desimaaliesitys, jonka esijakson pituus on N ja jaksonpituus $\lambda = \mathrm{ord}_U 10$, siten että N on pienin sellainen kokonaisluku, että $T \mid 10^N$. Osoitetaan, että esijakson pituus ja jaksonpituus eivät voi olla pienempiä kuin N ja λ.

Oletetaan, että $\alpha = 0, q_1 q_2 \ldots q_M \overline{q_{M+1} q_{M+2} \ldots q_{M+k}}$. Todistetaan, että $N \leq M$ ja $\lambda \leq k$. Nyt

$$
\begin{aligned}
\alpha =& 0, q_1 q_2 \ldots q_M \overline{q_{M+1} q_{M+2} \ldots q_{M+k}} \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_M}{10^M} + \frac{q_{M+1}}{10^{M+1}} + \frac{q_{M+2}}{10^{M+2}} + \cdots + \frac{q_{M+k}}{10^{M+k}} \\
&+ \frac{q_{M+k+1}}{10^{M+k+1}} + \cdots + \frac{q_{M+k+k}}{10^{M+k+k}} + \frac{q_{M+2k+1}}{10^{M+2k+1}} + \cdots + \frac{q_{M+2k+k}}{10^{M+2k+k}} + \frac{q_{M+3k+1}}{10^{M+3k+1}} + \cdots \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_M}{10^M} + \left(\sum_{j=0}^{\infty} \left(\frac{1}{10^k} \right)^j \right) \left(\frac{q_{M+1}}{10^{M+1}} + \frac{q_{M+2}}{10^{M+2}} + \cdots + \frac{q_{M+k}}{10^{M+k}} \right) \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_M}{10^M} + \left(\frac{1}{1 - \frac{1}{10^k}} \right) \left(\frac{q_{M+1}}{10^{M+1}} + \frac{q_{M+2}}{10^{M+2}} + \cdots + \frac{q_{M+k}}{10^{M+k}} \right) \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_M}{10^M} + \left(\frac{1}{\frac{10^k - 1}{10^k}} \right) \left(\frac{q_{M+1}}{10^{M+1}} + \frac{q_{M+2}}{10^{M+2}} + \cdots + \frac{q_{M+k}}{10^{M+k}} \right) \\
=& \frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_M}{10^M} + \left(\frac{10^k}{10^k - 1} \right) \left(\frac{q_{M+1}}{10^{M+1}} + \frac{q_{M+2}}{10^{M+2}} + \cdots + \frac{q_{M+k}}{10^{M+k}} \right) \\
=& \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_M}{10^M} \right) \frac{10^M (10^k - 1)}{10^M (10^k - 1)} \\
&+ \left(\frac{10^k}{10^k - 1} \right) \left(\frac{q_{M+1}}{10^{M+1}} + \frac{q_{M+2}}{10^{M+2}} + \cdots + \frac{q_{M+k}}{10^{M+k}} \right) \\
=& \frac{(q_1 10^{M-1} + q_2 10^{M-2} + \cdots + q_M)(10^k - 1)}{10^M (10^k - 1)} + \frac{q_{M+1} 10^{k-1} + q_{M+2} 10^{k-2} + \cdots + q_{M+k}}{10^M (10^k - 1)} \\
=& \frac{(q_1 10^{M-1} + q_2 10^{M-2} + \cdots + q_M)(10^k - 1) + q_{M+1} 10^{k-1} + q_{M+2} 10^{k-2} + \cdots + q_{M+k}}{10^M (10^k - 1)} \\
=& \frac{r}{s}.
\end{aligned}
$$

Luku α on rationaalilukuna muotoa $\alpha = \frac{r}{s}$, missä r ja s ovat keskenään jaottomia kokonaislukuja ja s on muotoa $s = TU$, missä $T = 2^u 5^v$, missä $u, v = 0, 1, 2, \ldots$, ja $\mathrm{syt}(U, 10) = 1$. Näin ollen $s \mid 10^M (10^k - 1)$, joten $T \mid 10^M$ ja $U \mid (10^k - 1)$. Koska $T \mid 10^M$, on oltava $M \geq N$, koska N on oletuksen mukaan pienin sellainen positiivinen kokonaisluku, että $T \mid 10^N$. Täten esijakson pituus ei voi olla pienempi kuin N.

Koska $U \mid (10^k - 1)$, seuraa tästä lauseen 2.2 perusteella, että $\mathrm{ord}_U 10 \mid k$, eli $\lambda \mid k$. Näin ollen jakson pituus ei voi olla pienempi kuin λ. □

Lauseen 3.3 perusteella voidaan määrittää desimaaliesityksen esijakson pituus ja jaksonpituus.

Esimerkki 3.5. Esimerkkejä esijakson pituuksista ja jaksonpituuksista:

(i) Rationaaliluvun
$$\frac{3}{28} = \frac{3}{2^2 \cdot 5^0 \cdot 7} = 0,10\overline{714285}$$
esijakson pituus $N = \max\{0, 2\} = 2$ ja jaksonpituus $\lambda = \text{ord}_7 10 = 6$, sillä
$$\begin{aligned} 10^6 &\equiv 1 \pmod 7, \quad \text{ja} \\ 10^x &\not\equiv 1 \pmod 7, \quad \text{kun} \quad x = 1, 2, \ldots, 5. \end{aligned}$$

(ii) Rationaaliluvun
$$\frac{1}{18} = \frac{1}{2^1 \cdot 5^0 \cdot 9} = 0,0\overline{5}$$
esijakson pituus $N = \max\{0, 1\} = 1$ ja jaksonpituus $\lambda = \text{ord}_9 10 = 1$, sillä
$$10^1 \equiv 1 \pmod 9.$$

(iii) Rationaaliluvun
$$\frac{5}{84} = \frac{5}{2^2 \cdot 5^0 \cdot 21} = 0,05\overline{952380}$$
esijakson pituus $N = \max\{0, 2\} = 2$ ja jaksonpituus $\lambda = \text{ord}_{21} 10 = 6$, sillä
$$\begin{aligned} 10^6 &\equiv 1 \pmod{21}, \quad \text{ja} \\ 10^x &\not\equiv 1 \pmod{21}, \quad \text{kun} \quad x = 1, 2, \ldots, 5. \end{aligned}$$

3.3 Algebraa ja lukuteoriaa

Määritelmä 3.4. [6] Olkoon m positiivinen kokonaisluku. Kokonaisluvun *a jäännösluokka modulo m* on joukko
$$[a]_m = \{b \in \mathbb{Z} \mid b \equiv a \pmod m\}.$$

Jäännösluokka modulo m voidaan myös kirjoittaa muodossa
$$[a]_m = \{a + km \mid k \in \mathbb{Z}\}.$$

Lukua a kutsutaan jäännösluokan $[a]_m$ *edustajaksi*.

Esimerkki 3.6. Esimerkkejä jäännösluokista modulo 11:
$$\begin{aligned} [1]_{11} &= \{\ldots, -21, -10, 1, 12, 23, \ldots\} \\ [5]_{11} &= \{\ldots, -17, -6, 5, 16, 27, \ldots\} \\ [7]_{11} &= \{\ldots, -15, -4, 7, 18, 29, \ldots\}. \end{aligned}$$

Jäännösluokkien joukko modulo m on
$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}.$$

Esimerkki 3.7. Kaikkien jäännösluokkien joukko modulo 11 on

$$\mathbb{Z}_{11} = \{[0]_{11}, [1]_{11}, [2]_{11}, \ldots, [10]_{11}\}.$$

Jäännösluokan $[a]_m \in \mathbb{Z}_m$ edustajana voi toimia mikä tahansa luku, joka on kongruentti luvun a kanssa modulo m, eli mikä tahansa jäännösluokan alkio.

Esimerkki 3.8. Jäännösluokat $[-10]_{11}$, $[1]_{11}$ ja $[12]_{11}$ ovat samat, sillä

$$\begin{aligned} -10 &\equiv 1 \pmod{11} \\ 1 &\equiv 12 \pmod{11}. \end{aligned}$$

Jäännösluokkien joukko $\mathbb{Z}_m$ voidaan yhtä hyvin kirjoittaa muodossa.

$$\mathbb{Z}_m = \{[1]_m, [2]_m, \ldots, [m-1]_m, [m]_m\},$$

sillä

$$[0]_m = [m]_m,$$

koska

$$0 \equiv m \pmod{m}.$$

Lause 3.4. *Jäännösluokkien joukossa $\mathbb{Z}_m$ voidaan määritellä yhteenlasku*

$$[a]_m \oplus [b]_m = [a+b]_m.$$

Todistus. [4, s. 118] Oletetaan, että $[a]_m = [a']_m$ ja $[b]_m = [b']_m$ joillakin $a, a', b, b' \in \mathbb{Z}$. Tällöin

$$\begin{aligned} a &\equiv a' \pmod{m} \\ b &\equiv b' \pmod{m}. \end{aligned}$$

Tällöin on olemassa luvut $k, l \in \mathbb{Z}$, joille pätee

$$\begin{aligned} a &= a' + km \\ b &= b' + lm. \end{aligned}$$

Laskemalla nämä puolittain yhteen saadaan

$$\begin{aligned} a + b &= a' + km + b' + lm \\ &= (a' + b') + (k + l)m, \end{aligned}$$

mistä seuraa, että

$$a + b \equiv a' + b' \pmod{m}.$$

Siis

$$[a+b]_m = [a' + b']_m.$$

□

Lause 3.5. *Jäännösluokkien joukossa $\mathbb{Z}_m$ voidaan määritellä kertolasku*

$$[a]_m \otimes [b]_m = [ab]_m.$$

Todistus. [4, s. 119] Oletetaan, että $[a]_m = [a']_m$ ja $[b]_m = [b']_m$ joillakin $a, a', b, b' \in \mathbb{Z}$. Tällöin

$$\begin{aligned} a &\equiv a' \pmod{m} \\ b &\equiv b' \pmod{m}. \end{aligned}$$

Tällöin on olemassa luvut $k, l \in \mathbb{Z}$, joille pätee

$$\begin{aligned} a &= a' + km \\ b &= b' + lm. \end{aligned}$$

Kertomalla nämä puolittain saadaan

$$\begin{aligned} ab &= (a' + km)(b' + lm) \\ &= a'b' + a'lm + kmb' + kmlm \\ &= a'b' + (a'l + kb' + klm)m, \end{aligned}$$

mistä seuraa, että

$$ab \equiv a'b' \pmod{m}.$$

Siis

$$[ab]_m = [a'b']_m.$$

□

Määritelmä 3.5. [6] Jäännösluokkaa $[a]_m$ sanotaan *alkuluokaksi* modulo m, mikäli $\text{syt}(a, m) = 1$. Kaikkien alkuluokkien joukko modulo m on joukko

$$\mathbb{Z}_m^\times = \{[a]_m \in \mathbb{Z}_m \mid syt(a, m) = 1\}.$$

Määritelmä 3.6. [7, s. 161] *Eulerin ϕ-funktion* arvo $\phi(m)$ on niiden kokonaislukujen $1 \leq a \leq m$ lukumäärä, joille $\text{syt}(a, m) = 1$. Ts. Eulerin funktio ϕ määritellään kaavalla

$$\phi(m) = |\{a \in \mathbb{Z} : 1 \leq a \leq m,\ \text{syt}(a, m) = 1\}|, \qquad m \in \mathbb{Z}^+.$$

Eulerin ϕ-funktion arvo $\phi(m)$ voidaan määrittää seuraavien lauseiden avulla.

Lause 3.6. *Jos m on alkuluku, niin $\phi(m) = m - 1$. Vastaavasti, mikäli m on positiivinen kokonaisluku, jolle $\phi(m) = m - 1$, niin m on alkuluku.*

Todistus. [7, s. 167] Todistus sivuutetaan. □

Lause 3.7. *Olkoon $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ positiivisen kokonaisluvun $m \geq 2$ alkulukuhajotelma. Tällöin*

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Todistus. [7, s. 169] Todistus sivuutetaan. □

Esimerkki 3.9. Esimerkkejä Eulerin ϕ-funktion arvoista:

(i) Koska luku 19 on alkuluku, niin lauseen 3.6 perusteella luvun 19 Eulerin ϕ-funktion arvo on

$$\phi(19) = 18.$$

(i) Luvun $4312 = 2^3 7^2 11$ Eulerin ϕ-funktion arvo saadaan lauseesta 3.7

$$\begin{aligned}\phi(4312) &= 4312(1 - \frac{1}{2})(1 - \frac{1}{7})(1 - \frac{1}{11}) \\ &= 4312 \cdot \frac{1}{2} \cdot \frac{6}{7} \cdot \frac{10}{11} \\ &= 1680.\end{aligned}$$

Määritelmien 3.5 sekä 3.6 perusteella Eulerin ϕ-funktion arvo $\phi(m)$ on myös joukon $\mathbb{Z}_m^\times$ alkioiden lukumäärä.

Esimerkki 3.10. Alkuluokkien joukko modulo 9, joukon alkioiden lukumäärä sekä Eulerin ϕ-funktion arvo $\phi(9)$ ovat:

$$\begin{aligned}\mathbb{Z}_9^\times &= \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\} \\ \left|\mathbb{Z}_9^\times\right| &= 6 \\ \phi(9) &= 9(1 - \frac{1}{3}) = 9 \cdot \frac{2}{3} = 6.\end{aligned}$$

Lause 3.8. [1, s. 42] *Pari* $(\mathbb{Z}_m^\times, \otimes)$ *on Abelin ryhmä.*

Todistus. Joukko $\mathbb{Z}_m^\times$ varustettuna laskutoimituksella $\otimes$ on Abelin ryhmä, mikäli seuraavat ehdot ovat voimassa: (i) laskutoimitus $\otimes$ on määritelty joukossa $\mathbb{Z}_m^\times$, (ii) laskutoimitus $\otimes$ on liitännäinen, (iii) laskutoimitus $\otimes$ on vaihdannainen, (iv) joukossa $\mathbb{Z}_m^\times$ on neutraalialkio laskutoimitukselle $\otimes$ ja (v) jokaisella joukon $\mathbb{Z}_m^\times$ alkiolla on käänteisalkio laskutoimituksen $\otimes$ suhteen.

(i) Olkoot $[a]_m, [b]_m \in \mathbb{Z}_m^\times$. Nyt $[a]_m \otimes [b]_m = [ab]_m$. Koska $\text{syt}(a, m) = 1$ ja $\text{syt}(b, m) = 1$, myös $\text{syt}(ab, m) = 1$, ja näin ollen $[ab]_m \in \mathbb{Z}_m^\times$. Koska $[ab]_m = [a]_m \otimes [b]_m$, niin myös $[a]_m \otimes [b]_m \in \mathbb{Z}_m^\times$.

(ii) Olkoot $[a]_m, [b]_m, [c]_m \in \mathbb{Z}_m^\times$. Silloin

$$\begin{aligned}([a]_m \otimes [b]_m) \otimes [c]_m &= [ab]_m \otimes [c]_m \\ &= [(ab)c]_m \\ &= [a(bc)]_m \\ &= [a]_m \otimes [bc]_m \\ &= [a]_m \otimes ([b]_m \otimes [c]_m),\end{aligned}$$

koska $(ab)c = a(bc)$.

(iii) Olkoon $[a]_m, [b]_m \in \mathbb{Z}_m^\times$. Nyt

$$[a]_m \otimes [b]_m = [ab]_m = [ba]_m = [b]_m \otimes [a]_m,$$

koska $ab = ba$. Eli laskutoimitus $\otimes$ on vaihdannainen.

(iv) Alkio $[1]_m \in \mathbb{Z}_m^\times$, sillä $\text{syt}(1, m) = 1$. Laskutoimituksen $\otimes$ neutraalialkio on $[1]_m$, sillä

$$[a]_m \otimes [1]_m = [a1]_m = [a]_m$$

aina, kun $[a]_m \in \mathbb{Z}_m^\times$.

(v) Olkoon $[a]_m \in \mathbb{Z}_m^\times$. Todistetaan, että alkiolla $[a]_m$ on käänteisalkio, eli että on olemassa sellainen $[x]_m \in \mathbb{Z}_m^\times$, että $[a]_m \otimes [x]_m = [1]_m$. Nyt $[ax]_m = [1]_m$, joka voidaan kirjoittaa muodossa $ax \equiv 1 \pmod{m}$. Lauseen 2.3 perusteella tällä kongruenssiyhtälöllä on kokonaislukuratkaisu, jos ja vain jos $\text{syt}(x, m) \mid 1$ eli $\text{syt}(x, m) = 1$. Siis $[x]_m \in \mathbb{Z}_m^\times$ ja alkiolla $[a]_m$ on käänteisalkio $[x]_m$ joukossa $\mathbb{Z}_m^\times$.

□

Lause 3.9. *Olkoot a, $m > 0$, olkoon $\text{syt}(a, m) = 1$ ja olkoot $i, j \geq 0$. Tällöin*

$$a^i \equiv a^j \pmod{m} \iff i \equiv j \pmod{\text{ord}_m a}.$$

Todistus. [3, s. 16]

(i) " $\Longleftarrow$ ": Oletetaan ensin, että $i \equiv j \pmod{\text{ord}_m a}$. Voidaan myös rajoituksetta olettaa, että $0 \leq j \leq i$. Oletuksesta saadaan, että

$$i = j + k(\text{ord}_m a), \quad k \in \mathbb{Z}_+.$$

Koska $\equiv$ on ekvivalenssirelaatio, on se refleksiivinen. Tällöin saadaan, että

$$\begin{aligned} a^i &\equiv a^i && \pmod{m} \\ a^i &\equiv a^{j+k(\text{ord}_m a)} && \pmod{m} \\ a^i &\equiv a^j a^{k(\text{ord}_m a)} && \pmod{m} \\ a^i &\equiv a^j (a^{\text{ord}_m a})^k && \pmod{m}. \end{aligned} \tag{3.6}$$

Määritelmän 2.3 ja kongruenssin laskusääntöjen avulla saadaan, että

$$\begin{aligned} a^{\text{ord}_m a} &\equiv 1 && \pmod{m} \\ (a^{\text{ord}_m a})^k &\equiv 1^k && \pmod{m} \\ a^j (a^{\text{ord}_m a})^k &\equiv a^j \cdot 1^k = a^j && \pmod{m}. \end{aligned} \tag{3.7}$$

Kaavojen (3.6) ja (3.7) perusteella saadaan, että

$$\begin{aligned} a^i &\equiv a^j (a^{\text{ord}_m a})^k && \pmod{m} \\ a^j (a^{\text{ord}_m a})^k &\equiv a^j && \pmod{m}, \end{aligned}$$

mistä seuraa kongruenssin transitiivisuuden perusteella, että

$$a^i \equiv a^j \pmod{m}.$$

" $\Longrightarrow$ ": Oletetaan sitten, että $a^i \equiv a^j \pmod{m}$. Koska $\text{syt}(a, m) = 1$, on myös $\text{syt}(a^j, m) = 1$. Tällöin voidaan käyttää kongruenssin supistussääntöä. Siis

$$\begin{aligned}
a^i &\equiv a^j && \pmod{m} && \\
a^{i+j-j} &\equiv a^j && \pmod{m} && \\
a^j a^{i-j} &\equiv a^j && \pmod{m} && \parallel \text{ supistussääntö} \\
a^{i-j} &\equiv 1 && \pmod{m}. &&
\end{aligned}$$

Lauseen 2.2 mukaan on oltava $\text{ord}_m a \mid (i - j)$. Siis

$$\begin{aligned}
i - j &= k\text{ord}_m a, \qquad k \in \mathbb{Z} \\
i &= j + k\text{ord}_m a, \qquad k \in \mathbb{Z} \\
i &\equiv j \pmod{\text{ord}_m a}.
\end{aligned}$$

□

Lause 3.10. Jakoyhtälö: *Olkoot a ja b kokonaislukuja ja olkoon $b > 0$. Tällöin on olemassa sellaiset yksikäsitteiset q, $r \in \mathbb{Z}$, $0 \leq r < b$, että $a = bq + r$.*

Todistus. [8, s. 13] Todistetaan (i) lukujen a ja r olemassaolo ja (ii) niiden yksikäsitteisyys.

(i) Oletetaan, että reaaliluku $\frac{a}{b} = q + \epsilon$, missä q on kokonaisluku ja $0 \leq \epsilon < 1$. Tällöin

$$a = b(q + \epsilon) = bq + b\epsilon.$$

Luvut a, b ja q ovat kokonaislukuja, niin myös bq on kokonaisluku. Näin ollen myös luvun $b\epsilon$ on oltava kokonaisluku. Koska $0 \leq \epsilon < 1$, niin $0 \leq b\epsilon < b$. Merkitään $r = b\epsilon$. Siis luvut q ja r ovat olemassa.

(ii) Oletetaan, että

$$\begin{aligned}
&(3.8) && a = bq + r, && 0 \leq r < b \\
&(3.9) && a = bq' + r', && 0 \leq r' < b.
\end{aligned}$$

Vähentämällä yhtälöt puolittain saadaan

$$\begin{aligned}
a - a &= (bq + r) - (bq' + r') \\
0 &= bq - bq' + r - r' \\
r' - r &= b(q - q') \\
(3.10) \qquad \frac{r' - r}{b} &= q - q'.
\end{aligned}$$

Muokkaamalla kaavojen (3.8) ja (3.9) epäyhtälöitä saadaan $-b < -r \leq 0$ ja $0 \leq r' < b$. Yhdistämällä nämä ja jakamalla puolittain luvulla $b > 0$ saadaan

$$-b < r' - r < b$$
$$-1 < \frac{r' - r}{b} < 1. \tag{3.11}$$

Koska luvut q ja q' ovat kokonaislukuja, kaavan (3.10) perusteella myös luku $\frac{r'-r}{b}$ on kokonaisluku. Kaavan (3.11) perusteella kyseinen kokonaisluku on suurempi kuin -1 ja pienempi kuin 1. Tällöin ainoa mahdollisuus on, että

$$\frac{r' - r}{b} = 0. \tag{3.12}$$

Koska $b > 0$, on oltava $r' - r = 0$. Yhdistämällä tämä tieto kaavaan (3.10) saadaan, että $q - q' = 0$. Näistä seuraa, että

$$r = r'$$
$$q = q'.$$

□

Lukua q kutsutaan osamääräksi ja lukua r jäännökseksi.

Rationaaliluvun desimaaliesitys voidaan löytää jakokulman avulla, joka perustuu jakoalgoritmiin.

3.3.1 Muotoa $\frac{1}{b}$ olevat rationaaliluvut

Tämä aliluku pohjautuu valtaosin lähteeseen [5]. Tarkastellaan muotoa $\frac{1}{b}$ olevan rationaaliluvun jakokulmalaskua ja osamäärien q_n sekä jäännöksien r_n, $n = 0, 1, 2, \ldots$, muodostumista seuraavan esimerkin avulla.

Esimerkki 3.11. Rationaaliluvun $\frac{1}{13}$ jakokulmalasku.

$$\begin{array}{r|l}
 & 0,0\,7\,6\,9\ \cdots \\
13 & 1,0\,0\,0\,0\ \cdots \\
\cline{2-2}
 & 0 \\
 & \underline{1\ 0} \\
 & \ \ 0 \\
 & \underline{1\ 0\ 0} \\
 & \ \ 9\ 1 \\
 & \underline{\ \ \ 9\ 0} \\
 & \ \ \ 7\ 8 \\
 & \underline{\ \ 1\ 2\ 0} \\
 & \ \ 1\ 1\ 7 \\
 & \underline{\ \ \ \ \ 3} \\
 & \ \ \ \ \ \vdots
\end{array}$$

Sinisellä merkityt luvut muodostavat osamäärien jonon $q_0, q_1, q_2, \ldots$, ja punaisella merkityt luvut muodostavat jakojäännöksien jonon $r_0, r_1, r_2, \ldots$

Muotoa $\frac{1}{b}$ olevan rationaaliluvun, missä $\text{syt}(b, 10) = 1$, jakojäännökset r_n toteuttavat rekursion

$$\begin{aligned} 10r_n &= bq_{n+1} + r_{n+1}, \quad n = 0, 1, \ldots \\ r_0 &= 1, \end{aligned} \tag{3.13}$$

mistä saadaan, että

$$\begin{aligned} 10r_n &\equiv r_{n+1} \pmod{b} \quad n = 0, 1, \ldots \\ r_0 &= 1. \end{aligned} \tag{3.14}$$

Esimerkki 3.12. Tarkastellaan esimerkin 3.11 osamääriä ja jakojäännöksiä kaavan (3.13) avulla, kun $r_0 = 1$ ja $q_0 = 0$:

$$\begin{aligned} 10r_0 &= 13q_1 + r_1 && \text{eli} && 10 \cdot 1 = 13 \cdot 0 + 10 \\ 10r_1 &= 13q_2 + r_2 && \text{eli} && 10 \cdot 10 = 13 \cdot 7 + 9 \\ 10r_2 &= 13q_3 + r_3 && \text{eli} && 10 \cdot 9 = 13 \cdot 6 + 12 \\ 10r_3 &= 13q_4 + r_4 && \text{eli} && 10 \cdot 12 = 13 \cdot 9 + 13. \\ &\vdots && && \vdots \end{aligned}$$

Käyttämällä hyväksi kaavaa (3.14) ja kongruenssin laskusääntöjä voidaan kirjoittaa

$$\begin{aligned} r_n &\equiv 10r_{n-1} && \pmod{b} && && \\ r_{n-1} &\equiv 10r_{n-2} && \pmod{b} && \therefore \quad 10r_{n-1} &\equiv 10 \cdot 10r_{n-2} && \pmod{b} \\ r_{n-2} &\equiv 10r_{n-3} && \pmod{b} && \therefore \quad 10^2 r_{n-2} &\equiv 10^2 \cdot 10r_{n-3} && \pmod{b} \\ r_{n-3} &\equiv 10r_{n-4} && \pmod{b} && \therefore \quad 10^3 r_{n-3} &\equiv 10^3 \cdot 10r_{n-4} && \pmod{b} \\ &\vdots && && && \vdots && \\ r_2 &\equiv 10r_1 && \pmod{b} && \therefore \quad 10^{n-2} r_2 &\equiv 10^{n-2} \cdot 10r_1 && \pmod{b} \\ r_1 &\equiv 10r_0 && \pmod{b} && \therefore \quad 10^{n-1} r_1 &\equiv 10^{n-1} \cdot 10r_0 && \pmod{b}. \end{aligned}$$

Yhdistämällä nämä saadaan

$$\begin{aligned} r_n &\equiv 10r_{n-1} \pmod{b} \\ &\equiv 10^2 r_{n-2} \pmod{b} \\ &\equiv 10^3 r_{n-3} \pmod{b} \\ &\vdots \\ &\equiv 10^{n-1} r_1 \pmod{b} \\ &\equiv 10^n r_0 \pmod{b}. \end{aligned}$$

Muotoa $\frac{1}{b}$ olevalle rationaaliluvulle on $r_0 = 1$, jolloin saadaan

$$r_n \equiv 10^n \pmod{b}, \quad n = 0, 1, \ldots \tag{3.15}$$

Määritelmän 2.3 mukaan luvun a kertaluku $x > 0$ modulo b on pienin sellainen kokonaisluku, että

$$a^x \equiv 1 \pmod{b}.$$

Olkoon $\text{syt}(10, b) = 1$. Merkitään luvun 10 kertalukua modulo b seuraavasti: $l = \text{ord}_b 10$. Tällöin $10^l \equiv 1 \pmod{b}$. Toisaalta kaavaan (3.15) mukaan $r_n \equiv 10^n \pmod{b}$. Kongruenssin transitiivisuuden perusteella näistä seuraa, että

$$r_l \equiv 1 \pmod{b}.$$

Jakojäännösten jonossa $r_1, r_2, \ldots r_l, r_{l+1}, r_{l+2}, \ldots$ luku $l = \text{ord}_b 10$ on jakojäännösten jonon jaksonpituus.

Lause 3.11. *Rationaaliluvun $\frac{1}{b}$, missä $\text{syt}(b, 10) = 1$, jakolaskun jakojäännöksille r_n pätee $r_{l+n} \equiv 10^n \pmod{b}$, missä l on luvun 10 kertaluku modulo b.*

Todistus. Olkoon luku $l = \text{ord}_b 10$ luvun 10 kertaluku modulo b. Määritelmän 2.3 mukaan tällöin $10^l \equiv 1 \pmod{b}$. Näin ollen

$$\begin{aligned} 10^l &\equiv 1 \pmod{b} \quad \| \cdot 10^n \\ 10^l \cdot 10^n &\equiv 1 \cdot 10^n \pmod{b} \\ 10^{l+n} &\equiv 10^n \pmod{b}. \end{aligned} \tag{3.16}$$

Kaavoista (3.15) ja (3.16) saadaan kongruenssin transitiivisuuden perusteella

$$r_{l+n} \equiv 10^n \pmod{b}.$$

□

Esimerkki 3.13. Olkoon $l = \text{ord}_{17} 10 = 16$. Esimerkkejä rationaaliluvun $\frac{1}{17}$ jakojäännöksistä: $r_3 = 14, r_{10} = 2, r_{3+16} = 14, r_{10+16} = 2$. Kaavasta (3.15) sekä lauseesta 3.11 saadaan, että

$$\begin{aligned} r_3 &\equiv 10^3 \pmod{17} \\ r_{19} &\equiv 10^3 \pmod{17} \\ r_{10} &\equiv 10^{10} \pmod{17} \\ r_{26} &\equiv 10^{10} \pmod{17}. \end{aligned}$$

Lauseen 3.11 sekä kaavan (3.15) perusteella tapauksen $\frac{1}{b}$ jakojäännökset r_n ovat kongruentteja lukujen 10^x kanssa seuraavasti:

$$\begin{aligned}
r_0 &\equiv 1 \pmod{b} \\
r_1 &\equiv 10 \pmod{b} \\
r_2 &\equiv 10^2 \pmod{b} \\
&\vdots \\
r_{l-1} &\equiv 10^{l-1} \pmod{b} \\
r_l &\equiv 1 \pmod{b} \\
r_{l+1} &\equiv 10^1 \pmod{b} \\
r_{l+2} &\equiv 10^2 \pmod{b} \\
&\vdots
\end{aligned}$$

Tapauksen $\frac{1}{b}$ jakojäännöksien r_n muodostama jäännösluokkien modulo b joukko on

$$L = \{[r_0]_b, [r_1]_b, [r_2]_b, \ldots, [r_{l-1}]_b\}.$$

Korvataan jäännösluokkien edustajat r_n niiden kanssa kongruenteilla luvuilla modulo b, jolloin jakojäännöksiä vastaavien jäännösluokkien modulo b joukoksi saadaan

$$L = \{[1]_b, [10]_b, [10^2]_b, \ldots, [10^{l-1}]_b\}.$$

Luku l on jakojäännösten jonon jaksonpituus. Lisäksi l on joukon L alkioiden lukumäärä määritelmän 2.3 perusteella.

Lause 3.12. *Muotoa $\frac{1}{b}$, missä* $\mathrm{syt}(b, 10)$*, olevan rationaaliluvun desimaaliesityksen jaksonpituus λ on yhtä suuri kuin jakojäännösten r_n muodostaman jonon jaksonpituus l.*

Todistus. Lauseen 3.3 perusteella muotoa $\frac{r}{s} = \frac{r}{TU}$, $\mathrm{syt}(r, s) = syt(U, 10) = 1$, olevan rationaaliluvun desimaaliesityksen jaksonpituus $\lambda = \mathrm{ord}_U 10$, kun $U > 1$. Kun $r = T = 1$ saadaan muotoa $\frac{1}{U}$ oleva rationaaliluku, jonka jakojäännösten r_n muodostaman jonon jaksonpituus $l = \mathrm{ord}_U 10$. Siis $\lambda = l$. □

Lause 3.13. *Pari $(L, \otimes)$ on ryhmän $(\mathbb{Z}_b^\times, \otimes)$ aliryhmä, missä L on jakojäännöksiä r_n vastaavien jäännösluokkien modulo b joukko.*

Todistus. Äärellisten ryhmien aliryhmäkriteerin mukaan pari $(L, \otimes)$ on ryhmän $(\mathbb{Z}_b^\times, \otimes)$ aliryhmä, mikäli (i) $\emptyset \neq L \subseteq \mathbb{Z}_b^\times$ (ii) $\forall\, [c]_b, [d]_b \in L : [c]_b \otimes [d]_b \in L$.

(i) Koska $\mathrm{syt}(b, 10) = 1$, myös $\mathrm{syt}(b, 10^n) = 1$ aina, kun $n \in \mathbb{Z}_+ \cup \{0\}$. Näin ollen $\mathrm{syt}(b, 10^n) = 1$, kun $n = 0, 1, \ldots, l-1$. Siis $[10^n]_b \in \mathbb{Z}_b^\times$, joten L on joukon $\mathbb{Z}_b^\times$ epätyhjä osajoukko.

(ii) Olkoon $[c]_b = [10^i]_b$ ja $[d]_b = [10^j]_b$, $0 \leq i, j \leq l$. Tällöin lauseen 3.9 perusteella

$$[10^i]_b \otimes [10^j]_b = [10^{i+j}]_b = [10^n]_b \in L,$$

missä n on luvun $i + j$ jäännös modulo l. Näin ollen $n < l$, joten $[10^n]_b \in L$. Täten kertolasku $\otimes$ on sulkeutuva joukossa L.

Pari $(L, \otimes)$ on siis ryhmän $(\mathbb{Z}_b^\times, \otimes)$ aliryhmä. □

Lause 3.14. *Rationaaliluvun $\frac{1}{b}$, missä* $\text{syt}(b, 10) = 1$*, desimaaliesityksen jaksonpituus λ jakaa Eulerin ϕ-funktion arvon $\phi(b)$.*

Todistus. Koska $\text{syt}(b, 10) = 1$, niin rationaaliluvun $\frac{1}{b}$ desimaalieistys on jaksollinen. Olkoon $\lambda > 0$ desimaaliesityksen jaksonpituus. Määritelmistä 3.5 ja 3.6 saadaan, että alkuluokkaryhmän alkioiden lukumäärä $\left|\mathbb{Z}_b^\times\right|$ on sama kuin Eulerin funktion arvo $\phi(b)$. Olkoon $L = \{[r_0]_b, [r_1]_b, [r_2]_b, \ldots, [r_{l-1}]_b\}$ jakojäännöksistä r_n muodostettujen alkuluokkien joukko, joka on alkuluokkaryhmän $\mathbb{Z}_b^\times$ aliryhmä. Jaksonpituus λ on lauseen 3.12 perusteella yhtä suuri kuin jakojäännösten r_n muodostaman jonon jaksonpituus l, joka on yhtä suuri kuin joukon L alkioiden lukumäärä. Lauseen 2.4 mukaan

$$|L| \,\Big|\, \left|\mathbb{Z}_b^\times\right|.$$

Siis

$$\lambda \Big| \phi(b).$$

□

Esimerkki 3.14. Tarkastellaan jakokulmalaskuja $\frac{1}{21}$.

$$
\begin{array}{r|llllllllll}
 & 0, & 0 & 4 & 7 & 6 & 1 & 9 & 0 & 4 & \cdots \\ \hline
21 & 1, & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
 & 0 & & & & & & & & & \\ \cline{2-2}
 & 1 & 0 & & & & & & & & \\
 & & 0 & & & & & & & & \\ \cline{2-3}
 & 1 & 0 & 0 & & & & & & & \\
 & & 8 & 4 & & & & & & & \\ \cline{2-4}
 & & 1 & 6 & 0 & & & & & & \\
 & & 1 & 4 & 7 & & & & & & \\ \cline{3-5}
 & & & 1 & 3 & 0 & & & & & \\
 & & & 1 & 2 & 6 & & & & & \\ \cline{4-6}
 & & & & & 4 & 0 & & & & \\
 & & & & & 2 & 1 & & & & \\ \cline{6-7}
 & & & & & 1 & 9 & 0 & & & \\
 & & & & & 1 & 8 & 9 & & & \\ \cline{6-8}
 & & & & & & & 1 & 0 & & \\
 & & & & & & & & 0 & & \\ \cline{8-9}
 & & & & & & & 1 & 0 & 0 & \\
 & & & & & & & & 8 & 4 & \\ \cline{8-10}
 & & & & & & & & 1 & 6 & \\
 & & & & & & & & & \vdots &
\end{array}
$$

Alkuluokkien joukko modulo 21 on

$$\mathbb{Z}_{21}^{\times} = \{[1]_{21}, [2]_{21}, [4]_{21}, [5]_{21}, [8]_{21}, [10]_{21}, [11]_{21}, [13]_{21}, [16]_{21}, [17]_{21}, [19]_{21}, [20]_{21}\}.$$

Eulerin funktion arvo luvulle 21 on $\phi(21) = 12$, eli alkuluokkaryhmän $\mathbb{Z}_{21}^{\times}$ alkioiden lukumäärä on myös 12. Jakojäännöksistä r_n muodostettujen alkuluokkien joukko on

$$L = \{[1]_{21}, [4]_{21}, [10]_{21}, [13]_{21}, [16]_{21}, [19]_{21}\}.$$

Korvataan jakojäännöksien r_n edustajat niiden kanssa kongruenteilla luvuilla modulo 21 seuraavasti:

$$
\begin{aligned}
1 &\equiv 10^0 \pmod{21} \\
4 &\equiv 10^4 \pmod{21} \\
10 &\equiv 10^1 \pmod{21} \\
13 &\equiv 10^3 \pmod{21} \\
16 &\equiv 10^2 \pmod{21} \\
19 &\equiv 10^5 \pmod{21},
\end{aligned}
$$

jolloin jakojäännöksiä vastaavien jäännösluokkien joukoksi modulo 21 saadaan

$$L = \{[10^0]_{21}, [10^1]_{21}, [10^2]_{21}, [10^3]_{21}, [10^4]_{21}, [10^5]_{21}\}.$$

3.3.2 Muotoa $\frac{c}{b}$ olevat rationaaliluvut

Verrataan muotoa $\frac{1}{b}$, missä $\text{syt}(b, 10) = 1$, ja $\frac{c}{b}$, missä $\text{syt}(b, 10) = 1$, olevien rationaalilukujen jakojäännöksiä esimerkin avulla. Aihetta on tarkasteltu yleisemmällä tasolla tarkemmin lähteessä [5, s. 14]

Esimerkki 3.15. Tarkastellaan jakokulmalaskuja $\frac{1}{21}$ ja $\frac{2}{21}$. Esimerkissä 3.14 on esitetty rationaalilukuvun $\frac{1}{21}$ jakokulmalasku.

$$
\begin{array}{rl}
 & 0,0\,9\,5\,2\,3\,8\,0\,9\ \cdots \\
\cline{2-2}
21 & \big| \ 2,0\,0\,0\,0\,0\,0\,0\,0\,0\ \cdots \\
 & 0 \\
\cline{2-2}
 & 2\ 0 \\
 & \ \ 0 \\
\cline{2-2}
 & 2\ 0\ 0 \\
 & 1\ 8\ 9 \\
\cline{2-3}
 & \ \ 1\ 1\ 0 \\
 & \ \ 1\ 0\ 5 \\
\cline{2-4}
 & \ \ \ \ \ 5\ 0 \\
 & \ \ \ \ \ 4\ 2 \\
\cline{2-5}
 & \ \ \ \ \ \ 8\ 0 \\
 & \ \ \ \ \ \ 6\ 3 \\
\cline{2-6}
 & \ \ \ \ \ \ 1\ 7\ 0 \\
 & \ \ \ \ \ \ 1\ 6\ 8 \\
\cline{2-7}
 & \ \ \ \ \ \ \ \ \ 2\ 0 \\
 & \ \ \ \ \ \ \ \ \ \ \ 0 \\
\cline{2-8}
 & \ \ \ \ \ \ \ \ \ 2\ 0\ 0 \\
 & \ \ \ \ \ \ \ \ \ 1\ 8\ 9 \\
\cline{2-9}
 & \ \ \ \ \ \ \ \ \ \ \ 1\ 1 \\
 & \ \ \ \ \ \ \ \ \ \ \ \ \ \vdots
\end{array}
$$

$$
\begin{aligned}
\phi(21) &= 12 \\
\mathbb{Z}_{21}^{\times} &= \{[1]_{21}, [2]_{21}, [4]_{21}, [5]_{21}, [8]_{21}, [10]_{21}, [11]_{21}, [13]_{21}, [16]_{21}, [17]_{21}, [19]_{21}, \\
&\quad [20]_{21}\} \\
L &= \{[1]_{21}, [4]_{21}, [10]_{21}, [13]_{21}, [16]_{21}, [19]_{21}\} \\
[2]_{21} \otimes L &= [2]_{21} \otimes \{[1]_{21}, [4]_{21}, [10]_{21}, [13]_{21}, [16]_{21}, [19]_{21}\} \\
&= \{[2 \cdot 1]_{21}, [2 \cdot 4]_{21}, [2 \cdot 10]_{21}, [2 \cdot 13]_{21}, [2 \cdot 16]_{21}, [2 \cdot 19]_{21}\} \\
&= \{[2]_{21}, [8]_{21}, [20]_{21}, [26]_{21}, [32]_{21}, [38]_{21}\} \\
&= \{[2]_{21}, [5]_{21}, [8]_{21}, [11]_{21}, [17]_{21}, [20]_{21}\}
\end{aligned}
$$

Lauseen 3.13 perusteella pari $(L, \otimes)$ on parin $(\mathbb{Z}_{21}^{\times}, \otimes)$ aliryhmä. Joukko $[2]_{21} \otimes L$ on alkion $[2]_{21}$ määräämä vasen sivuluokka modulo L. Kaikki vasemmat sivuluokat

$[c]_{21} \otimes L$ saadaan, kun $[c]_{21}$ käy läpi kaikki ryhmän $\mathbb{Z}_{21}^{\times}$ alkiot. Kaikki vasemmat sivuluokat muodostavat joukon $\mathbb{Z}_{21}^{\times}$ osituksen. Joukolla $\mathbb{Z}_{21}^{\times}$ on lauseen 2.5 perusteella $\frac{|\mathbb{Z}_{21}^{\times}|}{|L|} = \frac{12}{6} = 2$ vasenta sivuluokkaa:

$$[1]_{21} \otimes L = \{[1]_{21}, [4]_{21}, [10]_{21}, [13]_{21}, [16]_{21}, [19]_{21}\}$$
$$[2]_{21} \otimes L = \{[2]_{21}, [5]_{21}, [8]_{21}, [11]_{21}, [17]_{21}, [20]_{21}\}.$$

Mikäli alkio $[c]_{21}$ kuuluu joukkoon L, on alkion $[c]_{21}$ määräämä vasen sivuluokka on $[c]_{21} \otimes L = L$. Näin ollen kaikilla muotoa $\frac{c}{21}$, missä $[c]_{21} \in L$, olevilla rationaaliluvuilla on samat jakojäännökset kuin rationaaliluvulla $\frac{1}{21}$, eli rationaalilukujen desimaaliesityksien jaksot muodostuvat samoista luvuista, jotka esiintyvät samassa järjestyksessä. Jakson ensimmäinen luku määräytyy ensimmäisestä jakojäännöksestä. Mikäli alkio $[c]_{21}$ kuuluu joukkoon $\mathbb{Z}_{21}^{\times}$ mutta ei joukkoon L, on $[c]_{21} \otimes L = [2]_{21} \otimes L$, ja muotoa $\frac{c}{21}$ olevilla rationaaliluvuilla on samat jakojäännökset kuin rationaaliluvulla $\frac{2}{21}$, eli niiden desimaaliesityksien jaksot muodostuvat samoista luvuista, jotka esiintyvät samassa järjestyksessä. Jakson ensimmäinen luku määräytyy ensimmäisen jakojäännöksen perusteella.

Lähteet

[1] Haukkanen, P. *Algebra I*. Tampereen yliopisto, 2004. http://www.sis.uta.fi/matematiikka/arkisto/algebra/algI04.pdf. Viitattu 14.6.2015.

[2] Haukkanen, P. *Algebra II*. Tampereen yliopisto, 2004. http://www.sis.uta.fi/matematiikka/arkisto/algebra/algII04.pdf. Viitattu 27.6.2015.

[3] Haukkanen, P. *Lukuteoriaa*. http://www.sis.uta.fi/matematiikka/arkisto/algebra/Lukuteoria/lukuteoria.pdf. Viitattu 30.6.2015.

[4] Häsä, J., Rämö, J. *Johdatus abstraktiin algebraan*, 1. painos. Gaudeamus, 2012.

[5] Poranen, J., Haukkanen, P. *Jaksolliset desimaaliesitykset algebrallisesta näkökulmasta*. Tampereen yliopisto. http://matematiikkalehtisolmu.fi/2011/Poranen-Haukkanen.pdf. Viitattu 16.5.2015.

[6] Ranto, S. *Lukuteorian ja algebran digitaalinen oppimateriaali*. Turun yliopisto, 2003. https://matta.hut.fi/matta/algebra/algebra.html. Viitattu 14.6.2015.

[7] Rosen, K. H. *Elementary Number Theory and Its Applications*, 1. painos. Addison-Wesley, 1986.

[8] Vanden Eynden, C. *Elementary Number Theory*, 1. painos. The Random House/Birkhäuser Mathematics Series, 1987.